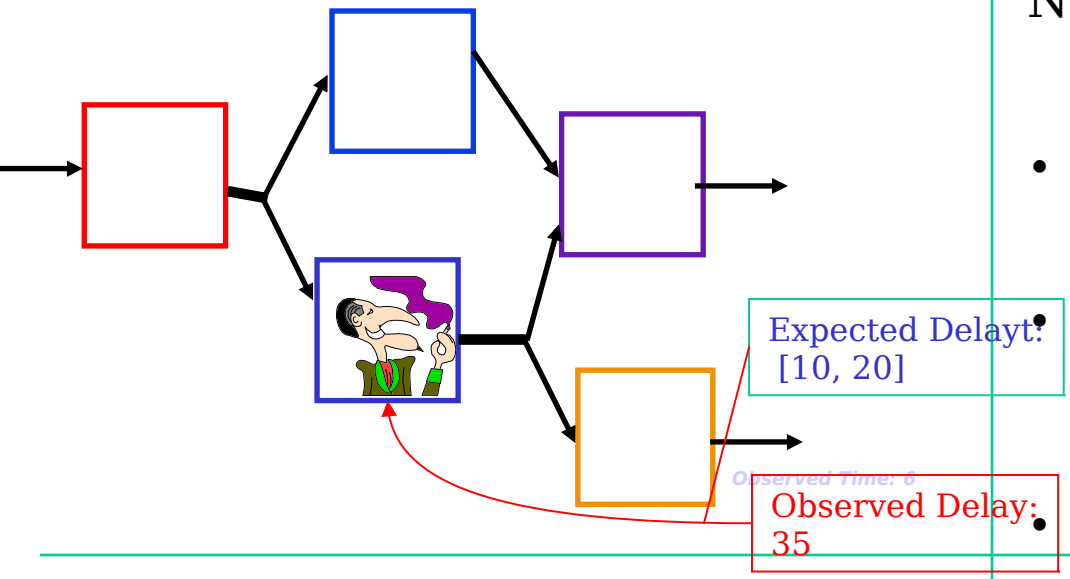
Ensuring Survivable Information Services

Model Based Intrusion Detection



New Ideas: Symptom guided Intrusion & Compromise Detection:

- System Modeling language describes both functionality and Quality of Service
- Model-based troubleshooting algorithms isolate candidates and characterize the form of compromise..
- Diagnosis guides the selection of a recovery plan which allows the application to recover and continue with its mission.

Impact:

- 50% reduction in false negatives rate for intrusion detection.
- Order of magnitude improvement in the precision of diagnosing intrusions and compromises
- Enables for the first time a coordinated approach to detecting intrusions and enabling the application system to recover from compromise.

Schedule

1. Develop System Modeling Language for use in Model Based Diagnosis (Oct 1998)
2. Develop model of simple pipelined signal processing system (Apr 1999)
3. Demonstrate Prototype Model Based Diagnosis system for this system (Aug 1999)
4. Demonstrate Ability to detect a compromise under laboratory conditions (Sep 1999)

MIT Artificial Intelligence Laboratory: Howard Shrobe, Randall Davis